REMARKS

This application has been carefully considered in connection with the Examiner's Final Office Action dated May 2, 2007. Reconsideration and allowance are respectfully requested in view of the following.

Summary of Rejections

Claims 1, 5, 7, 8, 10, 11, 13, 14, 18-25, 30 and 32-45 were pending at the time of the Final Office Action.

Claims 1, 5, and 38-40 were rejected under 35 U.S.C. 103(a) as being unpatentable over Dadhia et al., U.S. Patent Publication No. 2005/0188419 (hereinafter "Dadhia") in view of Linetsky, U.S. Patent Publication No. 2005/0138433 (hereinafter "Linetsky").

Claims 7, 8, 10, 11, 13, 21-23, 41-43 were rejected under 35 USC 103(a) as being unpatentable over Dadhia in view of Linetsky in view of Magruire et al., U.S. Patent Publication No. 2003/0208606 (hereinafter "Maguire").

Claims 24-25 were rejected under 35 USC 103(a) as being unpatentable over Dadhia in view of Linetsky in view of Magurie and further in view of Freund, U.S. Patent 5,987,611 (hereinafter "Freund").

Claims 14, 18-20, 44-45 were rejected under 35 USC 103(a) as being unpatentable over Dadhia.

Claims 30, 32-33 were rejected under 35 USC 103(a) as being unpatentable over Dadhia in view of Freund.

Claim 34 was rejected under 35 USC 103(a) as being unpatentable over Dadhia in view of Freund and further in view of Linetsky and Maguire.

Claims 35-37 were rejected under 35 USC 103(a) as being unpatentable over Dadhia in view of Linetsky and further in view of Maguire.

Summary of Response

Claims 1, 5, 7, 8, 10, 11, 13, 18, 23-25, 30, 32-45 were previously presented.

Claims 19 and 20 remain as originally submitted.

Claims 14, 21 and 22 have been amended.

Claims 2-4, 6, 9, 12, 15-17, 26-29, and 31 have been canceled.

Remarks and Arguments are provided below.

Summary of Claims Pending

Claims 1, 5, 7-8, 10-11, 13-14, 18-25, 30, and 32-45 are currently pending following this response.

Response to Rejections

The pending disclosure is generally related to remediated computer networks and systems and methods for protecting remediated computer networks from vulnerabilities of computer systems in the remediated network. In an embodiment of the disclosure, a computer system may raise a firewall upon the computer system physically connecting or reconnecting to a remediated computer network. Raising the

firewall upon connecting to the remediated computer network enables computer systems that are periodically disconnected from the remediated computer network to be remediated with scheduled or other pending remediations prior to the computer system gaining full access to the remediated computer network. The firewall may block all communications with the remediated computer network except for permitted communications with a component of the remediated computer network to remediate the computer system. The firewall may be maintained until the component of the remediated computer network remediates the computer system to verify that the computer system does not have any vulnerabilities. Utilizing a component of the remediated computer network to perform remediations for computer systems in the remediated computer network enables remediation of aggregated vulnerabilities. A detailed discussion of the differences between the claim limitations and the applied art follows.

Response to Rejections under 35 USC 103

In the Final Office Action dated May 2, 2007, Claims 1, 5, and 38-40 were rejected under 35 U.S.C. 103(a) as being unpatentable over Dadhia et al., U.S. Patent Publication No. 2005/0188419 (hereinafter "Dadhia") in view of Linetsky, U.S. Patent Publication No. 2005/0138433 (hereinafter "Linetsky").

Claim 1:

I. Dadhia does not disclose raising a firewall resident on the computer system **whenever** connecting or reconnecting said computer system.

Dadhia discloses in paragraph 0014 to establish limitations when an instance of an application first starts executing (i.e., startup). Dadhia discloses in paragraph 0018 that the limitations may be implemented by a firewall restricting access of the instances of the application to resources such as restricting the instance of the application from access to the Internet. Applicants note that the firewall of Dadhia is not raised whenever connecting to a remediated computer network. Rather, the firewall of Dadhia may be raised upon an instance of an application executing.

Dadhia also discloses in dependent claim 3 that determining the security level of an instance of an application is performed when the computer system connects to a network. Looking to independent claim 1, from which claim 3 depends, an action of a rule may be performed (i.e., establishing limitations) if the security level of an instance of an application satisfies a condition of the rule (i.e., the security level indicates the application is not up-to-date).

Claim 3 does not disclose establishing limitations on an instance of an application when the computer system connects to a network. Rather, implicit with the limitations of claim 1, if the condition of the rule isn't satisfied (i.e., the application is up-to-date) then the action of the rule is not performed (i.e., no limitations are placed on the instance of the application). This disclosure implicit to the claims is described in detail in paragraph 0014 of Dadhia. In particular, paragraph 0014 of Dadhia states, "If

an instance of an application is up-to-date, then the only overhead may be when the instance is started to see if any limitations need to be placed. Since none need to be placed, there may be no or very little overhead when resources are accessed by the instance."

It is clear from the disclosure of Dadhia that limitations, such as raising a firewall, are applied upon determining that the security level of an application is not up-to-date. While the determination of the security level of an application may take place at various times, such as upon starting an instance of the application or upon connecting to a network, this is not disclosure of raising a firewall whenever connecting or reconnecting a computer system as required by Claim 1. In contrast to Dadhia, Claim 1 requires the firewall to be raised regardless of whether the computer system requires remediation (i.e., "whenever").

II. Linetsky does not disclose raising a firewall resident on the computer system whenever connecting or reconnecting said computer system.

Applicant respectfully submits that the disclosure of Linetsky does not cure the deficiencies of Dadhia. Linetsky discloses a security methodology for defending against security breaches of peripheral devices (Linetsky: Abstract). In paragraph 0009, Linetsky discusses end point security systems that "may permit specific 'trusted' applications to access the Internet while denying access to other applications on a user's computer," similar to Dadhia. Linetsky discloses that such end point security systems are effective, however, in paragraph 0010 Linetsky discloses that such security systems do not provide security from detachable peripheral devices. Linestsky

discloses in paragraph 0014 that detachable peripheral devices pose two threats. The first threat is that communications between the peripheral device may be intercepted. The second threat is the peripheral device may be impersonated such that a computer may authenticate the peripheral device as legitimate when it is not legitimate. Linetsky discloses various ways of exploiting these threats in paragraphs 0010-0013.

Linetsky provides a solution for defending against security breaches of peripheral devices by requiring re-authentication of peripheral devices each time they are attached to the computer or each time the computer is restarted (paragraphs 0016 and 0053). Upon connection or reconnection of a peripheral device to a computer, the computer does not receive any input from the peripheral device (paragraphs 0050, 0055, and 0075). Linetsky discloses in paragraphs 0055-0057 that a peripheral device may be re-authenticated by a local or remote administrator entering a password. As a whole, Linetsky discloses a methodology for authenticating physical devices connected directly to a computer that may be used in addition to end point security systems such as Dadhia.

III. The combination of Linetsky and Dadhia would not result in the claim limitations.

While Linetsky does disclose in paragraph 0052 that the methodology may be applied to other peripheral devices, such as network cables, this disclosure does not provide any teaching or suggestion of raising a firewall on a computer whenever physically connecting the computer to a computer network as required by the claims. In particular, looking at Claim 1 as a whole, it is clear that the peripheral device

methodology disclosed by Linetsky would prevent some of the claimed limitations and would likewise prevent teachings of Dadhia.

For example, Claim 1 requires that the firewall which is raised on the computer to allow specified permitted communications while blocking all other communications. The Office Action relied on paragraphs 0018, 0019, and 0025 of Dadhia to teach this limitation. In paragraph 0025, for example, Dadhia discloses that "a limitation may be that the instance of the application has access only to a resource that will allow it to update to a more recent security level." Therefore, Dadhia requires limited communication with the network to allow an application to update. The methodology taught by Linetsky discloses to prevent all communication with a peripheral device until an administrator can re-authenticate it. This would prevent the application of Dadhia from updating.

While the security methodologies of Dadhia and Linetsky may be used in conjunction with one another, it is clear that the combination would not result in the claim limitations without the benefit of hindsight reconstruction. Applicants respectfully submit that the combination of Dadhia and Linetsky would result in a multi-layered security protection. For example, upon connecting a network cable to a computer, communication with the network cable may be blocked until an administrator can authenticate the network cable, in accordance with the disclosure of Linetsky. Upon the administrator authenticating the network cable, the security system of Dadhia may impose limitations on applications that are not up-to-date and only allow access to resources that may be used to update the application.

IV. Dadhia does not disclose determining if the computer system requires remediation, wherein the determination is performed by a component of the computer network.

The Office Action relied on paragraphs 0018 and 0025 to teach these limitations. Dadhia discloses in paragraph 0018 that the dynamic protection system "may download protection rules from servers of the developers of the applications." Similarly, paragraph 0025 discloses, "the instance of the application has access only to a resource that will allow it to update to a more recent security level." While the computer system may receive information for updating an application from a resource of the network, there is no teaching or suggestion of a resource of a network determining if remediation is required. Rather, Dadhia appears to disclose a determination of whether to place limitations on an instance of an application is performed by the computer system as disclosed in paragraph 0014.

V. Dadhia does not disclose physically connecting or reconnecting the computer.

Dadhia does not provide any teaching or suggestion of disconnecting a computer system 102 from either the network 104 or the internet 105 and subsequently reconnecting the computer system 102. Paragraph 0018 of Dadhia discloses the operation of the dynamic protection system 101 when the computers 102 are already connected to the network 104 and already have access to the internet 105. Paragraph 0018 also discloses, "A user computer that is not connected to a local area network also may use the dynamic protection system." Applicants note that this is merely disclosure that a stand-alone user computer 102 (such as Computer 1 as shown in Fig.

1) may use the dynamic protection system 101 without being part of a local area network. That is, a user computer 102 doesn't have to be a part of the local area network 104 in order to use the network protection system 101. Applicants respectfully submit that this is not disclosure of disconnecting a computer system 102 from either the network 104 or the internet 105 and subsequently reconnecting the computer system 102.

The Office Action indicated that accessing a network resource after startup as recited in claim 2 of Dadhia is a physical connection or reconnection to the network. In light of the disclosure of Dadhia, it is clear that "startup" as recited in claim 2 refers to starting execution of an instance of an application as disclosed in paragraph 0014. Therefore, the Office Action has equated starting an instance of an application and accessing a resource of a network to a physical connection with a network. Applicants respectfully disagree with this characterization of the disclosure of Dadhia.

Looking to paragraphs 0064-0067 of the pending disclosure, various exemplary physical disconnections are described. For example, physical disconnections may include powering down a computer, performing a cold disconnect from a physical network connection (i.e., docking station or network cable), or performing a hot disconnect from a physical network connection. In general, a physical disconnection from a network may be thought of as a disconnection where a computer is physically unable to communicate with the network (see paragraph 0065). Applicant respectfully submits that Dadhia does not disclose any such physical disconnection or reconnection.

Dependent claims 5 and 38-40 are similarly not taught or suggested for at least the reasons detailed in sections I-V above.

In the Final Office Action dated May 2, 2007, Claims 7, 8, 10, 11, 13, 21-23, 41-43 were rejected under 35 USC 103(a) as being unpatentable over Dadhia et al., U.S. Patent Publication No. 2005/0188419 in view of Linetsky, U.S. Patent Publication No. 2005/0138433, in view of Magruire et al., U.S. Patent Publication No. 2003/0208606 (hereinafter "Maguire").

Claim 7:

Claim 7 includes limitations similar to those discussed in sections I-III and V above. As such, the arguments discussed above in sections I-III and V are herein repeated for Claim 7.

VI. Dadhia does not disclose verifying the computer system by a remediation server in the computer network.

In the rejection of Claim 7, the Office Action did not address the limitations of "raising a firewall ... until said computer system has been verified by said remediation server" and "lowers the firewall upon said remediation server verifying said computer system." Similar to the argument in section IV, Dadhia does not disclose a remediation server, wherein the remediation server verifies the computer system as required by the claims. Applicant respectfully submits that the term "verifying" includes at least checking for pending remediations and executing the pending remediations as defined in dependent claims 8 and 11. As discussed in the argument in section IV, while the

computer system of Dadhia may receive information for updating an application from a resource of the network, there is no teaching or suggestion of the resource of the network verifying the computer system.

VII. Maguire does not cure the deficiencies of Dadhia and Linetsky.

Maguire discloses an isolation component 210 that acts as a "switch" to disengage communication between the computer and a network to prevent access to data resident of the device (paragraphs 0013-0014, 0025). Maguire discloses to utilize the isolation component 210 when the computer will be unattended for extended periods of time such as when an employee leaves for the night (paragraph 0006). Maguire does not provide any teaching or suggestion of raising a firewall resident on the computer system whenever connecting or reconnecting said computer system.

While Maguire does provide a list of exemplary peripheral devices 141 in paragraph 0022, Applicants respectfully submit that this "peripheral device" is not a peripheral device of a computer, as the term is used in Linetsky. Rather, the "peripheral devices" of Maguire are devices that are peripheral to the network 199 as illustrated in FIG. 1. While the list of peripheral devices in paragraph 0022 includes some devices that may be used as peripheral devices of a computer, such as a printer or a camera, Maguire clearly describes the peripheral device 141 as a "network-enabled device". In contrast, the peripheral devices of Linetsky are devices such as a keyboard, a network cable, or other peripheral device that may be monitored with malicious intent.

Dependent claims 8, 10, 11, 13, 41, and 42 are similarly not taught or suggested for at least the reasons detailed in sections I-III and V-VII above.

Claim 21:

Claim 21 includes limitations similar to those discussed in sections I-V and VII above. As such, the arguments discussed above in sections I-V and VII are herein repeated for Claim 21.

Dependent claims 22 and 23 are similarly not taught or suggested for at least the reasons detailed in sections I-V and VII above.

In the Final Office Action dated May 2, 2007, Claims 24-25 were rejected under 35 USC 103(a) as being unpatentable over Dadhia et al., U.S. Publication No. 2005/0188419 in view of Linetsky, U.S. Patent Publication No. 2005/0138433 in view of Magurie et al, U.S. Patent Publication No. 2003/0208606 and further in view of Freund, U.S. Patent 5,987,611 (hereinafter "Freund").

Claims Depending from Claim 21:

Dependent claims 24 and 25 are similarly not taught or suggested for at least the reasons detailed in sections I-V and VII above. Applicant respectfully submits that Freund does not cure the deficiencies of Dadhia, Linetsky, and Maguire.

In the Final Office Action dated May 2, 2007, Claims 14, 18-20, 44-45 were rejected under 35 USC 103(a) as being unpatentable over Dadhia et al., U.S. Patent Publication No. 2005/0188419.

Claim 14:

Claim 14 includes limitations similar to those discussed in sections I and V above. As such, the arguments discussed above in sections I and V are herein repeated for Claim 14.

VIII. Dadhia does not disclose performing a scan on said computer system with a component of said network.

Similar to the argument in section IV, Dadhia does not disclose performing a scan on the computer with a component of the network, wherein the firewall is lowered upon removing any nefarious software detected by the scan, as required by the claims. As discussed in the argument in section IV, while the computer system of Dadhia may receive information for updating an application from a resource of the network, there is no teaching or suggestion of the resource of the network scanning the computer system and removing nefarious software.

Dependent claims 18-20 and 43-45 are similarly not taught or suggested for at least the reasons detailed in sections I, V, and VIII above.

In the Final Office Action dated May 2, 2007, Claims 30, 32-33 were rejected under 35 USC 103(a) as being unpatentable over Dadhia et al, U.S. Patent Publication No. 2005/0188419 in view of Freund, U.S. Patent No. 5,987,611.

Claim 30:

Claim 30 includes limitations similar to those discussed in section VI above. As such, the arguments discussed above in section VI are herein repeated for Claim 30.

IX. Dadhia does not teach or suggest closing a firewall upon power-up of the computer and upon initiation of registration with a computer network.

The Office Action has characterized Dadhia's disclosure of an instance of an application accessing a network resource as reading on initiation of registration with a computer network. While initiation of registration with a computer network may include accessing a resource of the network, disclosure of accessing a resource of a network is not implicit and does not suggest performing initiation of registration with a computer network.

Assuming arguendo, even if Dadhia's disclosure does suggest initiation of registration with a computer network, Applicants note that Dadhia does not disclose to impose limitations (i.e., raise a firewall) **upon** accessing the network as discussed above in section I.

Further, the claim limitations require a two-fold requirement of powering-up the computer system. The Office Action characterized the "startup" limitation in claim 2 as teaching powering-up the computer system. In light of the disclosure of Dadhia, it is clear that "startup" as recited in claim 2 refers to starting execution of an instance of an

application as disclosed in paragraph 0014. Therefore, Dadhia does not disclose raising a firewall upon either of the conditions required in the claims, let alone both of them.

X. Dadhia does not teach or suggest verifying that the computer system meets standards of the network.

While Dadhia does disclose to ensure that standards of the computer system are met (i.e., all applications are up-to-date), Dadhia does not provide any teaching or suggestion of verifying that the computer system meets the standards of the network.

Freund does not cure the deficiencies of Dadhia discussed above.

Dependent claims 32 and 33 are similarly not taught or suggested for at least the reasons detailed in sections VI, IX, and X above.

In the Final Office Action dated May 2, 2007, Claim 34 was rejected under 35 USC 103(a) as being unpatentable over Dadhia et al., U.S. Patent Publication No. 2005/0188419 in view of Freund, U.S. Patent No. 5,987,611 and further in view of Linetsky, U.S. Patent Publication No. 2005/0138433 and Maguire et al., U.S. Patent Publication No. 2003/0208606.

Claims Depending from Claim 30:

Dependent claim 34 is similarly not taught or suggested for at least the reasons detailed in sections VI, IX, and X above. Also note the arguments presented in sections II, III, V, and VII.

In the Final Office Action dated May 2, 2007, Claims 35-37 were rejected under 35 USC 103 (a) as being unpatentable over Dadhia et al., U.S. Patent Publication No. 2005/0188419 in view of Linetsky, U.S. Patent Publication No. 2005/0138433 and further in view of Maguire et al., U.S. Patent Publication No. 2003/0208606.

Claims Depending From Claim 1:

Dependent claims 35-37 are similarly not taught or suggested for at least the reasons detailed in sections I-V above. Also note the arguments presented in section VII.

Further, Applicants respectfully traverse the Official Notice taken in Claim 37. Applicant(s) note that MPEP 2144.03(b) requires that if Official Notice is taken of a fact that is unsupported by documentary evidence that "the basis for such reasoning must be set forth explicitly. The examiner must provide specific factual findings predicate on sound technical and scientific reasoning to support his or her conclusion of common knowledge". Applicants respectfully submit that the general conclusion in the Office Action that scheduling patch updates is known and that it would have been obvious to "include performing remediations scheduled for the computer system subsequent to the computer system disconnecting from the computer network so as to perform automatic update without relying upon the user or administrator," does not meet the requirements set forth in the section of the MPEP cited above.

Applicants respectfully submit that this conclusion resulted from the use of improper hindsight reasoning. Applicants note paragraph 00065 of the pending disclosure teaches that when a computer system is disconnected from the network,

scheduled remediations may not be performed by the remediation server. Further, paragraph 00065 discloses, "Because the remediated computer system 26c is disconnected when the next scheduled remediation is to occur, the vulnerability in the remediation computer system 26c will remain unsolved. As a result, absent the network protection process disclosed herein, the vulnerability would place both the remediated computer system 26c and the entire remediated computer network 19 at risk to the particular adverse effects associated with that particular vulnerability."

Conclusion

Applicants respectfully submit that the present application is in condition for allowance for the reasons stated above. If the Examiner has any questions or comments or otherwise feels it would be helpful in expediting the application, he is encouraged to telephone the undersigned at (972) 731-2288.

The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 50-1515, Conley Rose..

Respectfully submitted,

Date: June 28, 2007

Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANTS

CONLEY ROSE, P.C.
5700 Granite Parkway, Suite 330
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)